

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK**

In re Qudian Inc. Securities Litigation

Master File No. 1:17-cv-09741-JMF

**PLAINTIFFS' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR  
RECONSIDERATION OF ORDER DISMISSING PLAINTIFFS' DATA BREACH  
CLAIMS ALLEGED IN THE CONSOLIDATED SECOND AMENDED CLASS ACTION  
COMPLAINT**

Pursuant to the Stipulation and Scheduling Order, 2019, ECF No. 192, Plaintiffs submit this memorandum in support of their motion for reconsideration of the Court’s September 27, 2019 Order dismissing the data breach claims alleged in the Consolidated Second Amended Class Action Complaint. *In re Qudian Inc. Sec. Litig.*, 2019 WL 4735376, at \*7-\*8 (S.D.N.Y. Sept. 27, 2019) (the “Order”).

## I. INTRODUCTION

The Order held that “in light of [Qudian’s] disclosures, it cannot be said that Plaintiffs plausibly identify a material misrepresentation with respect to Qudian’s statements concerning its data security protocols.” *Id.* at \*8. Plaintiffs respectfully request reconsideration of this holding. The Registration Statement’s generic risk warnings are materially misleading because Defendants failed to disclose that Qudian had *already* experienced a massive data breach in early 2017, prior to the initial public offering (“IPO”), with over one million student borrowers’ personal information leaked into the black market. ¶¶ 8, 76-82, 110-19, 139.<sup>1</sup> According to an investigative news report, the sale of student borrowers’ personal information continued throughout 2017, and those sales were ongoing as of November 20, 2017 (the article’s publication date)—one month after Qudian’s October 18, 2017 IPO. ¶ 111.<sup>2</sup>

---

<sup>1</sup> All references to “¶ \_\_” refer to paragraphs in the Plaintiffs’ Consolidated Second Amended Class Action Complaint (ECF No. 134).

<sup>2</sup> See also Blake Declaration, Ex. M (ECF No. 144-13) (certified translation of the November 20, 2017 article entitled “Suspected QUDIAN Data Leakage, Information of a Million of Students Available with CNY 100,000”) (“In the first half of this year, someone began to sell such data, saying that they were QUDIAN’s student data and can be sold by region and province. ... Recently, people who sell data have kept a low profile, and no longer sell it publicly. The data can be traded only after introduction by an acquaintance.”).

Simply put, Defendants’ warning that Qudian’s “security measures *could be breached*” is not only insufficient as a caution, it is itself materially misleading because Qudian’s systems *had already been breached* and “[c]autionary words about future risk cannot insulate from liability the failure to disclose that the risk has transpired.” *Rombach v. Chang*, 355 F.3d 164, 173 (2d Cir. 2004); *see also Meyer v. Jinkosolar Holdings Co.*, 761 F.3d 245, 251 (2d Cir. 2014) (“A generic warning of a risk will not suffice when undisclosed facts on the ground would substantially affect a reasonable investor’s calculations of probability.”).

## **II. RECONSIDERATION IS WARRANTED TO CORRECT AN ERROR**

Motions for reconsideration are governed principally by Federal Rule of Civil Procedure 59(e) and Local Civil Rule 6.3, which requires that the movant concisely set forth “the matters or controlling decisions which counsel believes the court has overlooked.” L.R. 6.3. “To prevail on a motion for reconsideration, the movant must identify an intervening change in controlling law, the availability of new evidence, or the need to correct a clear error or prevent manifest injustice.” *Virgin Atl. Airways, Ltd. v. Nat’l Mediation Bd.*, 956 F.2d 1245, 1255 (2d Cir. 1992). Reconsideration is appropriate where a court has overlooked a matter “that might reasonably be expected to alter” its conclusion or where there is otherwise “a need to correct a clear error or prevent manifest injustice.” *Small v. Nobel Biocare USA, LLC*, 2012 WL 952396, at \*1 (S.D.N.Y. Mar. 21, 2012) (citations omitted).

## **III. QUDIAN’S DATA BREACH STATEMENTS ARE MATERIALLY MISLEADING UNDER CONTROLLING SECOND CIRCUIT LAW**

A company’s risk disclosures are misleading where the company warns only that a risk may impact its business when that risk has already materialized. *See Jinkosolar*, 761 F.3d at 251; *Rombach*, 355 F.3d at 173. In *Jinkosolar*, the Second Circuit evaluated misleading

statements in registration statement that Jinkosolar, a Chinese solar panel manufacturer, issued for its May 2010 ADS offering. *Jinkosolar*, 761 F.3d at 247. Jinkosolar’s prospectus discussed pollution related to the company’s business, the applicability of Chinese environmental regulations and standards, the company’s steps to achieve compliance, and the consequences of non-compliance. *Id.* The Second Circuit concluded that Jinkosolar’s statements about pollution abatement and environmental monitoring, while technically true, were materially misleading. *Id.* at 251. The complaint alleged that in June 2010 Jinkosolar submitted a report to Chinese regulators about existing problems that, if proven, could give rise to an inference that these problems existed at the time of the offering but were undisclosed. *Id.* The Court concluded:

The failure to disclose these problems in the May prospectus could be found by a trier of fact to be an omission that renders misleading the comforting statements in the prospectus about compliance measures. ***This misleading omission is not cured by the additional statement that non-compliance with the environmental regulations may be very costly. Although this statement warned of a financial risk to the company from environmental violations, the failure to disclose then-ongoing and serious pollution violations would cause a reasonable investor to make an overly optimistic assessment of the risk. A generic warning of a risk will not suffice when undisclosed facts on the ground would substantially affect a reasonable investor’s calculations of probability.*** *Rombach v. Chang*, 355 F.3d 164, 173 (2d Cir. 2004) (“Cautionary words about future risk cannot insulate from liability the failure to disclose that the risk has transpired.”).

*Id.* (emphasis added). Similarly, here, Defendants’ statements regarding cybersecurity were materially misleading because they failed to disclose that Qudian ***had already experienced a breach in early 2017***, prior to the IPO, and ***that the negative consequences of this breach were ongoing at the time of the IPO***. The failure to disclose these facts would, undoubtedly, cause “a reasonable investor to make an overly optimistic assessment of the risk.” *Id.*<sup>3</sup>

---

<sup>3</sup> Tellingly, when a November 20, 2017 news article first disclosed the data breach, the price of Qudian’s shares dropped by 5.28% to close at \$20.08 per share, and continued to fall as more

The risk disclosure at issue, quoted in the Order, does not state that Qudian’s systems “might have been breached in the past,” as the Order states (2019 WL 4735376 at \*8), but rather, only that its systems hypothetically *could be* breached:

We collect, store and process certain personal and other sensitive data from our users, which makes us an attractive target and potentially vulnerable to cyber-attacks, computer viruses, physical or electronic break-ins or similar disruptions. While we have taken steps to protect the confidential information that we have access to, *our security measures could be breached*. Because techniques used to sabotage or obtain unauthorized access to systems change frequently and generally are not recognized until they are launched against a target, *we may be* unable to anticipate these techniques or to implement adequate preventative measures. Any accidental or willful security breaches or other unauthorized access to our system *could cause* confidential user information to be stolen and used for criminal purposes. Security breaches or unauthorized access to confidential information *could also expose us to liability* related to the loss of the information, time-consuming and expensive litigation and negative publicity. *If* security measures are breached because of third-party action, employee error, malfeasance or otherwise, or *if* design flaws in our technology infrastructure are exposed and exploited, our relationships with users *could be* severely damaged, *we could incur significant liability* and our business and operations could be adversely affected.

Cohen Decl., R.S. at 47 (emphasis added). Defendants’ statement that its “not always possible to identify and deter misconduct or errors by employees,” is misleading for the same reason—Qudian had *already* experienced a cybersecurity data breach where a significant number of student borrowers’ highly confidential personal information was downloaded by Qudian employees and sold on the black market before the IPO. *Id.* at 46; *see* ¶¶ 8, 76-82, 110-19, 139.

The Order wholly adopted Defendants’ argument that, when pages 33, 192, and 194 of the Registration Statement are stitched together, they constitute an adequate disclosure of the

---

negative news regarding the data breach and other issues entered the marketplace. This is strong evidence that the market was unaware of a preexisting data breach at Qudian, *i.e.*, that it was not disclosed in the Registration Statement. For the Court’s convenience, the relevant pages of the Registration Statement (“R.S.”), previously submitted to the Court, are re-attached to the Cohen Declaration.

data breach. *Compare* ECF No. 143 at 23 *with* ECF No. 187 at 15-16 (2019 WL 4735376 at \*8). That was clear error. Defendants cobble a disclosure together from different sections of the Registration Statement separated by **159 pages**, which is both highly artificial and ineffective: that synthetic “disclosure” simply does not disclose the breach or the ongoing negative consequences.

Specifically, in their Motion to Dismiss, Defendants argued: “Qudian also disclosed it was the subject of investigations that included an examination by the Beijing Rectification Office for compliance with regulations concerning ‘keeping proper custody of the data . . . of . . . borrowers,’ and that ‘there can be no assurance that we will be able to receive . . . final clearance.’” To be clear, the first portion quoted by Defendants appears on page 192 of the Registration Statement as part of a list of **twenty-three** separately numbered topics covered by the regulations, and the second portion is not specific to data security and occurs **159 pages earlier**, in the context of Qudian explaining that while it believes it should not be subject to the regulations at all, the regulators currently disagree, and may continue to do so. Cohen Decl., R.S. at 33. The page 33 disclosure that a subsidiary company received a rectification notice under the “Interim Online Lending Information Intermediary Measures” nowhere discusses the 2017 data breach, and does not even mention cybersecurity or cybersecurity remediation. Cohen Decl., R.S. at 33. Nor does this section of the Registration Statement, read in conjunction with the statements made **159 pages later** listing more than 23 topics covered by the regulations contain a disclosure of the 2017 data breach. Cohen Decl., R.S. at 192-94. The simple truth of the matter is that the data breach and its continuing consequences were never disclosed to investors, **anywhere**.

*In re Heartland Payment Sys., Inc. Sec. Litig.*, 2009 WL 4798148, at \*5 (D.N.J. Dec. 7, 2009), cited by Defendants and relied upon in the Order (2019 WL 4735376 at \*8), is inapposite. It is out-of-circuit authority that did not analyze the sufficiency of a registration statement's risk disclosures under the standard that controls this case.<sup>4</sup> The *Heartland* court concluded that “the cautionary statements in the Form 10-K—warning of the possibility of a breach and the consequences of such a breach—make clear that Heartland was not claiming that its security system was invulnerable.” *Heartland*, 2009 WL 4798148 at \*5. But the issue here is not whether Qudian's security systems were actually perfect and legally compliant, but whether it was misleading for Defendants to advise investors that a significant data breach **could be** possible when, in fact, a data breach **had already occurred and the consequences were ongoing**. Such misstatements/omissions clearly deprive investors of the ability to make informed calculations of risk probability. *Jinkosolar*, 761 F.3d at 251.

Second Circuit precedent dictates that Defendants' misstatements and omissions are actionable.<sup>5</sup> Defendants' failure to disclose the 2017 breach and continuing sale of student data

---

<sup>4</sup> *Heartland* analyzed fraud claims asserted under the Exchange Act and the court did not rely on any Second Circuit authority in its analysis.

<sup>5</sup> Numerous other opinions in this Circuit support the conclusion that Defendants' failure to disclose the 2017 breach and ongoing issues related thereto was materially misleading. *E.g.*, *In re Facebook, Inc. IPO Sec. & Derivative Litig.*, 986 F. Supp. 2d 487, 516 (S.D.N.Y. 2013) (finding risk disclosures misleading where Facebook's registration statement did not disclose that increased mobile usage and the company's product decisions **had already** had a negative impact on the company's revenues and revenue growth); *Dodona I, LLC v. Goldman, Sachs & Co.*, 847 F. Supp. 2d 624, 646 (S.D.N.Y. 2012) (“Since the Offering Circulars contained affirmative representations regarding the risks of investing, . . . Defendants had a duty to ensure that those statements were accurate and complete.”); *In re Am. Int'l Grp., Inc. 2008 Secs. Litig.*, 741 F. Supp. 2d 511, 531 (S.D.N.Y. 2010) (“[G]eneric risk disclosures are inadequate to shield defendants from liability for failing to disclose known specific risks.”); *In re Van der Moolen Holding N.V. Sec. Litig.*, 405 F. Supp. 2d 388, 400 (S.D.N.Y. 2005) (statements purporting to warn that a company's business “could” be negatively impacted “if” it failed to comply with

in the Registration Statement is an omission that renders misleading the comforting statements in the Registration Statement about cybersecurity measures and purportedly *hypothetical* (as opposed to realized) risks. *Jinkosolar*, 761 F.3d at 251. Moreover, the Registration Statement’s discussion of potential consequences of Chinese regulations that are unrelated to cybersecurity does not cure Defendants’ misleading statements. *Id.* Qudian’s risk warnings misleadingly represented that data breaches were merely *possible* when, in fact, such risk had already *materialized* at the time of the IPO.

#### IV. CONCLUSION

For the reasons set forth herein, Plaintiffs respectfully request that the Court vacate the dismissal of Plaintiffs’ data breach claims alleged in the Consolidated Second Amended Class Action Complaint ¶¶ 8, 76-82, 110-19, 139.

Respectfully submitted,

**GLANCY PRONGAY & MURRAY LLP**

Dated: November 8, 2019

By: s/ Joseph D. Cohen  
 Joseph D. Cohen  
 Jonathan M. Rotter  
 1925 Century Park East, Suite 2100  
 Los Angeles, CA 90067  
 Telephone: (310) 201-9150  
 Facsimile: (310) 201-9160  
 jcohen@glancylaw.com  
 jrotter@glancylaw.com

*Co-Lead Counsel for Plaintiffs*

---

industry regulations were materially misleading where the company was violating industry regulations at the time it issued those purported warnings); *In re Prudential Secs. Inc. Ltd. P’ship Litig.*, 930 F. Supp. 68, 72 (S.D.N.Y. 1996) (“[E]ven apparently specific risk disclosures like those in [a defendant company’s] prospectus are misleading if the risks are professionally stamped in internal undisclosed analyses . . . as significantly greater or more certain than those portrayed in the prospectus.”).



Jack I. Zwick (JZ-2514)  
225 Broadway, Suite 1440  
New York, New York 10007  
Telephone: (212) 385-1900  
Facsimile: (212) 385-1911  
jack@zwickfirm.com

*Co-Lead Counsel for Plaintiffs*

**PROOF OF SERVICE**

I, the undersigned say:

I am not a party to the above case and am over eighteen years old.

On November 8, 2019, I served true and correct copies of the foregoing document, by posting the document electronically to the ECF website of the United States District Court for the Southern District of New York, for receipt electronically by the parties listed on the Court's Service List.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on November 8, 2019.

*s/ Joseph D. Cohen*

Joseph D. Cohen